様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 １９ 日現在

機関番号：１５５０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2019
課題番号：１６Ｋ００１５６

研究課題名（和文）基底の学習を用いた情報ハイディング技術への展開

研究課題名（英文）Extention of Information Hiding Method using basis learning

研究代表者
川村　正樹（Kawamura, Masaki）

山口大学・大学院創成科学研究科　・准教授

研究者番号：６０３１４７９６

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：高画質で、画像加工に強い情報ハイディング技術を開発するために、２つの手法を提案した。１つは、不変特徴を利用する方法であり、幾何変換に強い特徴点の周辺に透かし情報を埋め込む。埋め込み方の改善や誤り訂正符号の導入により、透かし情報の誤りを減らすことができた。もう１つは、ニューラルネットワークを用いた手法である。この手法は内部で回転攻撃をシミュレートするネットワークをもち、回転耐性のあるステゴ画像を学習することができる。その結果、回転攻撃に強い埋め込み器と抽出器を構成することができた。

研究成果の学術的意義や社会的意義
個人がSNS等へ写真をアップロードする機会が増え、写真の不正利用が問題となっている。電子透かし法はこれらの問題を解決する有効な手段の１つである。写真が加工されたとしても、透かし情報が正しく抽出できることが望まれる。そのため、高画質で加工に強い透かし法が求められている。本研究では、ニューラルネットワークに回転攻撃を学習させることにより、幾何変換に強い埋め込み器と抽出器を構成できることを示した。これにより、写真の不正利用の対策に貢献できる。

研究成果の概要（英文）：In order to develop the information hiding method which has high image-quality and robustness against image processing, we proposed two methods. One is a method using invariant features. Watermarks are embedded into embedding area around feature points which are robust against geometric transform. The proposed method could reduce errors in the watermarks by improvement of embedding technique and error correcting codes. The other is a neural network. The proposed network has a rotation-attack simulator inside and can learn robust stego-images. As a result, we could construct robust embedder and extractor networks against the rotation attack.

研究分野：情報科学

キーワード：情報ハイディング　電子透かし　特徴点　ニューラルネットワーク　学習

１．研究開始当初の背景

情報ハイディング技術とは、著作情報をコンテンツに埋め込む電子透かし技術と、情報を埋め込んだ痕跡を隠すステガノグラフィ技術などの総称である。インターネットの普及に伴い、著作権の保護を如何に行うかが重要な課題になっている。特に、音楽や映像、漫画などを不法にアップロードする行為が後を絶たず、不正コピーが蔓延している。情報ハイディング技術は、マルチメディアコンテンツの認証や秘密情報保護のための中核技術として注目されている。しかしながら、画像電子透かしの分野では、画像の切り出しや拡大縮小など幾何攻撃や、データの圧縮やデータ形式の変換などの非幾何攻撃への耐性が弱いことが課題であり、完全な実用化には至っていない。

電子透かしの埋め込みには、離散コサイン変換（DCT）やウェーブレット変換などの直交変換を用い、周波数領域に埋め込む手法が行われてきた。これらの手法は、可逆変換であるため、画質の劣化を小さくできる利点がある。また、圧縮などの非幾何攻撃には耐性がある。しかしながら、埋め込み領域の座標や範囲が変化する幾何攻撃には耐性が低い問題がある。従って、幾何攻撃に耐性がある手法を開発することが必要である。

スケール不変特徴変換（ SIFT）や KAZE などの特徴量は、幾何変換に対して不変な特徴量である。画像を拡大縮小や回転しても、同じ特徴点が得られる性質がある。これを利用すると、幾何攻撃耐性を持たせることができる。画像処理では、原画像と変換画像の両方を利用して、特徴点のマッチングが行われ、対応点を知ることができる。しかしながら、電子透かしでは原画像を用いないブラインド復号によって、透かし情報を抽出しなければならない。そのため、対応点を知るだけではなく、拡大率や回転角を推定し、同期を取る必要がある。さらに、攻撃による劣化や、透かし情報の推定誤りは避けることができない。そこで、透かし情報を誤り訂正符号等で変換し、埋め込み情報を生成する必要がある。

前述のように画像処理による方法の他に、ニューラルネットワークの学習による方法が考えられる。近年のディープラーニングの成功から、深層学習や畳み込みニューラルネットワーク（ CNN ）に注目が集まっている。　CNN は視覚モデルの１つであるネオコグニトロンから発展したニューラルネットワークである。画像の位置ずれや回転、拡大縮小に強いパターン認識を行えることが知られている。　DCTなどの直交基底を用いた変換に対して、　CNN では基底（フィルタ）を学習により獲得する。これより、幾何変換に強い基底を用いて透かし情報を埋め込むことができる可能性がある。また、同期を取る必要がなくなる可能性もある。

２．研究の目的

本研究では、拡大縮小や回転などの幾何変換に強い電子透かし法を開発することを目指す。そのために、２つの課題を設定した。

（１）．不変特徴点を用いた同期による手法

（２）．ニューラルネットワークによる学習を用いた埋め込み手法

どちらの課題も情報ハイディング及びその評価基準（ IHC ）委員会が定める電子透かしの評価基準に基づいて評価を行った。　IHC では、埋め込み者、攻撃者、復号者のそれぞれのモデルが決められている。特に、攻撃者では、画像に対して、拡大縮小、回転、切り出し、圧縮を行うことが定められている。復号時には、攻撃者が用いたパラメータは不明であるとして、攻撃された画像から透かし情報を抽出することが求められている。また、抽出した透かし情報の誤り率も規定されている。実用的な電子透かし法とするためには、　IHC の基準に適合する手法を提案することが必要である。本研究の目的は、 IHC 評価基準を満たし、耐性の強い電子

透かし法を開発することである。

３．研究の方法

課題（１）では、拡大縮小攻撃については、画像の正規化により、対応することができている。難しい点は、回転攻撃である。そこで、 SIFTや KAZA などの特徴抽出器の中から電子透かし法に最適な手法を求めた。また、特徴点の周辺に埋め込み領域を構成するとき、回転同期を取る必要がある。回転同期の方法について検討した。透かし情報を誤り訂正符号により埋め込み情報に変換するが、誤り訂正能力を上げるには符号長を長くしなければならない。しかしながら、埋め込み量が増大すると、透かし情報が埋め込まれたステゴ画像の画質が低下してしまう。そのため、誤り訂正能力と画質のバランスを調整する必要がある。このように、 IHC 評価基準を満たすように手法を最適化した。

課題（２）では、まずニューラルネットワークの構造を検討する必要がある。原画像と透かし情報からステゴ画像を生成し、ステゴ画像から透かし情報を抽出するニューラルネットワークとして、砂時計型のネットワークを検討した。ニューラルネットワークでは、同一層内のニューロンの配置を定めることができない。従って、ステゴ画像を中間層に生成する場合、その並びを固定する工夫が必要である。次に、 CNN を用いる方法を検討した。ステゴ画像と原画像、及び透かし情報を入力し、学習することにより、透かし情報を抽出させる。様々な攻撃を加えたステゴ画像を用意することで、攻撃耐性を獲得できる可能性がある。さらに、敵対的生成ネットワーク（ GAN ）を導入することにより、ステゴ画像の画質の向上が見込まれる。また、 GAN を用いることにより、原画像とステゴ画像を識別するステガナリシスや改ざん検出に応用することも検討できる。以上のように、電子透かし法に適したニューラルネットワークの構造をいくつか検討していった。

４．研究成果

課題（１）では、特徴検出器と誤り訂正符号、及び、これらをまとめて IHCの基準を達成するための手法を検討、評価した。特徴検出器では、特徴点から得られるスケールが、画像の拡大率に比例することが望ましい。 SIFT, KAZA, A-KAZEの特徴量を調べた結果、 SIFT がもっとも適していることが分かった。 KAZEは高速化のため、拡大率に比例しない特徴点が多いと考えられる [深田，川村 EMM (2017) ，内田，川村 EMM (2017), Kawamura, Uchida, IIH-MSP (2017)] 。誤り訂正符号に関しては、符号長と誤り訂正能力の他に、埋め込んだ後のステゴ画像の画質に対する評価も行う必要がある。 IHCが定めるメッセージ長として 200 ビットを埋め込む場合について検討した [佐伯，野崎，川村 EMM (2017)] 。 LDPC符号を用いて、最適化した手法による結果は、電子情報通信学会英文誌に掲載されている [Hirata, Nozaki, Kawamura, IEICE (2017)] 。また、 IHCの評価基準を達成するために、回転角の推定方法や埋め込み領域の決定方法などの改良を行った [林，川村 , EMM(2019)] 。これらの成果は国際会議論文 ASPIPA に掲載されている [Hayashi, Kawamura, APSIPA ASC (2018)] 。

課題（２）では、電子透かし法に適したニューラルネットワークの構造を検討した。まずはじめに、砂時計型ニューラルネットワークを用いた。このニューラルネットワークは情報の圧縮と伸長を行うネットワークと知られている。 N次元の原画像と M次元の電子透かしから N次元のステゴ画像を生成する符号化器と、ステゴ画像から N次元の原画像と M次元の電子透かしを抽出する復号器を学習によって構成した。ステゴ画像を出力する中間層が最も少なく、

くびれているので砂時計型の構造をしている。ニューラルネットワークの結合の値を調べることで、どのような電子透かし法に対応する学習を行っているかを解析した [濱元，川村，EMM (2017,2018)] 。また、この成果は電子情報通信学会英文誌に掲載されている [Hamamoto, Kawamura, IEICE (2019)]。次に、 CNN を用いた方法を検討した。特に注目した関連研究は HiDDen [1] である。内部に攻撃をシミュレートするネットワークを持ち、攻撃耐性を持ったステゴ画像を生成することができる。また、 GAN を導入することによって、画質の向上も図れている。我々は、攻撃として彼らが導入していなかった回転攻撃をシミュレートする回路を導入し、回転耐性がある手法を提案した。 IHCの基準を満たすビット数の埋め込みはできていないが、一定のビット長ならば回転耐性を持たせることに成功した。この成果は電子情報通信学会英文誌に掲載されている [Hamamoto, Kawamura, IEICE (2020)]。

これらの課題以外にも成果を得ることができた。電子透かしモデルの性能を理論的に評価するために、可解な電子透かしモデルの構築を行ってきた。スペクトル拡散型電子透かし法は、CDMA モデルと画像修復モデルの合成として定式化できる。我々は統計力学の手法であるレプリカ法を用いて、電子透かしのビット誤りに関する性能評価を行った。この成果は Physical Review E に掲載されている [Kawamura, Hayashi, Uezu, Okada, Physical Rev. E (2019)]。

参考文献

[1] Zhu J., Kaplan R., Johnson J., Fei-Fei L. (2018) HiDDeN: Hiding Data With Deep Networks. In: Ferrari V., Hebert M., Sminchisescu C., Weiss Y. (eds) Computer Vision – ECCV 2018. ECCV 2018. Lecture Notes in Computer Science, vol 11219. Springer, Cham

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　0件／うちオープンアクセス　4件）

１．著者名 Ippei HAMAMOTO, Masaki KAWAMURA	４．巻 E103.D
２．論文標題 Neural Watermarking Method Including an Attack Simulator against Rotation and Compression Attacks	５．発行年 2020年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 33～41
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019MUP0007	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Kawamura Masaki, Hayashi Kao, Uezu Tatsuya, Okada Masato	４．巻 99
２．論文標題 Statistical mechanical evaluation of a spread-spectrum watermarking model with image restoration	５．発行年 2019年
３．雑誌名 Physical Review E	６．最初と最後の頁 62132
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevE.99.062132	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Ippei Hamamoto, Masaki Kawamura	４．巻 E102.D
２．論文標題 Image Watermarking Technique Using Embedder and Extractor Neural Networks	５．発行年 2019年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 19～30
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018MUP0006	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Nobuhiro HIRATA, Takayuki NOZAKI, Masaki KAWAMURA	４．巻 E100-D
２．論文標題 Image Watermarking Method Satisfying IHC by Using PEG LDPC Code	５．発行年 2017年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 13-23
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2016MUP0003	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Keiichi IWAMURA, Masaki KAWAMURA, Minoru KURIBAYASHI, Motoi IWATA, Hyunho KANG, Seiichi GOHSHI, and Akira NISHIMURA	４．巻 E100-D
２．論文標題 Information Hiding and its Criteria for Evaluation	５．発行年 2017年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 2-12
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2016MUI0001	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計21件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Masaki Kawamura, Kouta Uchida
２．発表標題 SIFT Feature-Based Watermarking Method Aimed at Achieving IHC Ver.5
３．学会等名 The Thirteenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2017)（国際学会）
４．発表年 2017年

１．発表者名 南後 建太，川村 正樹
２．発表標題 スクリーンショット時にURLを埋め込むiPhoneアプリの開発
３．学会等名 電子情報通信学会 技術報告，第5回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会
４．発表年 2020年

１．発表者名 横田 明音，川村 正樹
２．発表標題 フレーム間の類似性を利用したBSSに基づく動画像電子透かし法の提案
３．学会等名 電子情報通信学会 技術報告，第6回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会
４．発表年 2020年

１．発表者名
深田 和真，川村 正樹

２．発表標題
電子透かしにおける誤り訂正能力を改善するための連想記憶モデルの検討

３．学会等名
電子情報通信学会 技術報告，第6回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2020年

１．発表者名
Dhidhi Pambudi, Masaki Kawamura

２．発表標題
A New Spy-Inspired Metaheuristic Algorithm

３．学会等名
電子情報通信学会 総合大会

４．発表年
2020年

１．発表者名
Masato Hayashi, Masaki Kawamura

２．発表標題
Improved SIFT feature-based watermarking method for IHC ver. 5

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference 2018 (APSIPA ASC 2018)（国際学会）

４．発表年
2018年

１．発表者名
島名 祐樹，川村 正樹

２．発表標題
相互想起型連想記憶モデルを用いた多重Zero-Watermarking法の提案

３．学会等名
電子情報通信学会 技術報告，第5回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2019年

１．発表者名
林 誠人，川村 正樹

２．発表標題
ヒストグラムの最頻値を用いた埋め込み領域の回転角推定

３．学会等名
電子情報通信学会 技術報告，第5回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2019年

１．発表者名
濱元 一平，川村 正樹

２．発表標題
回転に堅牢な抽出器NNを導入したCNNによる電子透かし法

３．学会等名
電子情報通信学会 技術報告，第6回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2019年

１．発表者名
押川 晃寛，川村 正樹

２．発表標題
誤り訂正符号の訂正能力と連想記憶モデルの引き込み領域の関係

３．学会等名
電子情報通信学会 技術報告，第6回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2019年

１．発表者名
林華央，上江洌達也，川村正樹

２．発表標題
電子透かしモデルの統計力学的解析 ーAT安定性評価ー

３．学会等名
日本物理学会2018年秋季大会

４．発表年
2018年

１．発表者名
林華央，上江洌達也，川村正樹

２．発表標題
電子透かしモデルの統計力学的研究-パラメータ推定-

３．学会等名
日本物理学会第74回年次大会

４．発表年
2019年

１．発表者名
濱元 一平，川村 正樹

２．発表標題
ニューラルネットワークを用いた符号化器による電子透かし法

３．学会等名
電子情報通信学会 技術報告，第4回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2017年

１．発表者名
濱元 一平，川村 正樹

２．発表標題
ニューラルネットワークはどのような埋め込み法を学習するのか

３．学会等名
電子情報通信学会 技術報告，第6回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2017年

１．発表者名
林 誠人，川村 正樹

２．発表標題
SIFT特徴点に基づく電子透かし法の改善 ～変動拡大率の導入による特徴領域の歪み低減～

３．学会等名
電子情報通信学会 技術報告，第6回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2017年

１．発表者名
馬 金晶，川村 正樹

２．発表標題
Evaluation of scanned image tolerance by using spread spectrum digital watermarking with regression analysis

３．学会等名
電子情報通信学会，第1回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2016年

１．発表者名
岩本 拓也，川村 正樹

２．発表標題
テキスト分割によるPDFファイルに対する不可視電子透かし法の提案

３．学会等名
電子情報通信学会，第4回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2016年

１．発表者名
内田 洸太，川村 正樹

２．発表標題
SIFT特徴点を利用した電子透かし法のIHC ver.5に基づく耐性評価

３．学会等名
電子情報通信学会，第5回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2017年

１．発表者名
深田 有花，川村 正樹

２．発表標題
KAZE特徴量を導入した電子透かし法の検討

３．学会等名
電子情報通信学会，第6回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2017年

１．発表者名
佐伯 豊彦，野崎 隆之，川村 正樹

２．発表標題
多元LDPC符号を用いた電子透かし法とJPEG圧縮に対する評価

３．学会等名
電子情報通信学会，第6回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2017年

１．発表者名
岩本 拓也，川村 正樹

２．発表標題
相対テキスト長パターンに基づくPDF文書に対する電子透かし法

３．学会等名
電子情報通信学会，第6回マルチメディア情報ハイディング・エンリッチメント（EMM）研究会

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

研究業績
http://www.is.sci.yamaguchi-u.ac.jp/~kawamura/Japanese/papers/

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考